REMARKS

Claims 43-62 are pending in the present application. Claims 43-62 stand rejected under 35 USC 103(a) as being unpatentable over US Pat. Publ. No. 2002/0004902 to Toh et al. (hereinafter "Toh") in view of U.S. Patent No. 5,781,629 to Haber et a. (hereinafter "Haber"). Applicant respectfully disagrees with the Examiner's analysis of the pending claims. However, in order to advance prosecution, Applicant has replaced the pending claims with new claims 63-72. Applicant reserves the right to pursue the subject matter of the cancelled claims without prejudice or disclaimer in one or more continuation applications.

New claim 63 is directed to a method of authenticating data including, *inter alia*,

> "… (b) generating a first data file comprising a respective hash value of each said plurality of stored data items;
> (c) **generating a single hash value of said first data file derived from said hash values of said plurality of stored data items**;
> (d) **transmitting said single hash value to a remote location, via an information technology communications network**;
> (e) creating at said remote location a second data file comprising said single hash value and one or more additional data items relating to said single hash value;
> (f) generating a hash value for said second data file;
> (g) **publishing said hash value for said second data file in a dated journal of record published in numerous copies and held in separate public libraries**; and
> (h) authenticating said second data file by generating a hash value for said second data file and comparing the hash value for the second data file generated in (h) with the hash value for said second data file published in said dated journal (emphasis added)."

Nowhere does the cited prior art teach or suggest these features.

Toh employs a hash algorithm on random data to generate a hash that is encrypted together with a sender's private key and sent along with a data package from a sender to an operations center. The operations center uses the sender's public key to decrypt the hash value received from the sender, utilizes the same hash algorithm on the original random data to derive a hash value, and checks that the decrypted hash value matches the derived hash value in order to authenticate that the sender sent the message. Importantly, Toh does not address the use of hash values to authentic a number of data items, let alone the steps of (b) - (h) as recited in claim 63.

Haber does not remedy the shortcomings of Toh. More specifically, Haber describes a user transmitting a request 20 to a remote service bureau. The request includes a hash value 21 for a particular document F. Col. 5, line 12-15. In contrast, the operation of (b) of claim 63 generates a first data file comprising a respective hash value for a plurality of stored data items" and the operation of (c) generates a single hash value of said first data file derived from said hash values of said plurality of stored data items. In (d), the single hash value is transmitted to a remote location, via an information technology communications network. Thus, the present invention of claim 63 transmits to a remote location a single hash value derived from hash values for a plurality of stored data items, whereas Haber transmits to a remote location only a single hash value for particular document. Haber also fails to teach or suggest the operation of g) of claim 63 in **publishing said hash value for said second data file in a dated journal of record published in numerous copies and held in separate public libraries**. Importantly, these features enable efficient authentication of a number of data items generated and

stored at any particular time, such as a number of electronic documents generated and stored by an organization during a given audit period as described in pages 8 to 9 of the present application as filed.

Thus, the cited prior art fails to teach or suggest important limitations of claim 63. Accordingly, claim 63 is clearly patentable over the cited prior art.

The dependent claims 64-68 are patentable over the cited prior art for those reasons advanced above with respect to claim 63 from which they respectfully depend and for reciting additional features that are neither taught or suggested by the cited prior art.

New claim 69 is directed to a method of enabling proof by a third party both of transmission of a message from a sender to a receiver and receipt of said message by said receiver, which includes:

> "… the sender generating a first hash value of said message;
> the sender encrypting said message with a first secret key and producing a second hash value from said encrypted message;
> the sender encrypting said first secret key with a second secret key;
> the sender transmitting to the receiver said encrypted message, said encrypted first secret key and said first hash value;
> the sender transmitting said second hash value and said second secret key to said third party;
> the third party storing the transmitted second hash value and second secret key for audit purposes;
> the receiver receiving said encrypted message and generating a purported copy of said second hash value of said encrypted message;
> the receiver transmitting the purported copy of said second hash value to the third party;
> the third party checking that the purported copy matches said second hash value; and
> the third party then releasing said second key if a match is determined."

Nowhere does the cited prior art teach or suggest these features. Accordingly, claim 69 is clearly patentable over the cited prior art.

Dependent claim 70 is patentable over the cited prior art for those reasons advanced above with respect to claim 69 from which it respectfully depends and for reciting additional features that are neither taught or suggested by the cited prior art.

New claim 71 is directed to a method for verifying by a recipient the authenticity of use of an identifier by a sender, which includes:

> "…(i) identifying the communication of a message encrypted using a secret key unique to said sender from said sender to said recipient across an information technology communications network;
> (ii) accessing, in response to said identification, storage means containing information relating to the most recent message encrypted using said secret key which has occurred across said information technology communications network;
> (iii) obtaining confirmation from said sender that said most recent event is valid, and
> (iv) preventing further use of said secret key in the event that said confirmation is not received."

Nowhere does the cited prior art teach or suggest these features. Accordingly, claim 71 is clearly patentable over the cited prior art.

Dependent claim 72 is patentable over the cited prior art for those reasons advanced above with respect to claim 71 from which it respectfully depends and for reciting additional features that are neither taught or suggested by the cited prior art.

In light of all of the above, it is submitted that the claims are in order for allowance, and prompt allowance is earnestly requested. Should any issues remain outstanding, the Examiner is invited to call the undersigned attorney of record so that the case may proceed expeditiously to allowance.

Respectfully submitted,

/Jay P. Sbrollini/

Jay P. Sbrollini
Attorney for Applicant(s)

GORDON & JACOBSON, P.C.
60 Long Ridge Road
Suite 407
Stamford, CT 06902
Ph:(203) 323-1800

August 4, 2009